



May XX, 2017

[First Name][Last Name]  
[Street Address]  
[City], [State] [Zip Code]

### **Notice of Data Breach**

Dear [First Name] [Last Name]:

FastHealth is a contracted vendor of [Healthcare provider]. We provide healthcare clients with operational and website services, including online patient questionnaires. We are committed to protecting the security and confidentiality of our clients' and their patients' information. Regrettably, we are writing to inform you about an incident involving some of that information.

### **What Happened**

On December 21, 2016, FastHealth discovered suspicious code on a server. Upon learning of this, we immediately began an investigation and hired a leading computer security firm to assist. On January 24, 2017, the computer security firm determined that an unauthorized third party altered code on FastHealth's web server that was to capture certain information as it was being entered on FastHealth's online patient questionnaires from January 14, 2016 to December 20, 2016.

### **What Information Was Involved**

FastHealth's forensic investigation concluded on March 25, 2017, and we subsequently determined the information that may have been affected includes your name, address, email address, date of birth, health insurance information, patient account number, clinical information such as diagnosis and procedure type, medications, medical history, and Social Security number.

### **What You Can Do**

We have no indication that your information has been misused in any way; however, as a precaution, we wanted to notify you of this incident and assure you that we take it very seriously. Out of an abundance of caution, we are offering a complimentary one-year membership in Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. ProtectMyID Alert is completely free to you and enrolling in this program will not hurt your credit score. **For more information on ProtectMyID Alert, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take to protect yourself, please see the page that follows this letter.**

**What We Are Doing**

We sincerely apologize for any inconvenience or concern this may cause you. To help prevent something like this from happening in the future, we have removed the malicious code and continue to take steps to strengthen the security of our network.

**For More Information**

If you have any questions, please call 1-844-534-0814, Monday through Friday, from 9 a.m. to 9 p.m. EST (closed on U.S. observed holidays).

Sincerely,

A handwritten signature in blue ink, reading "Kevin A. Foote". The signature is written in a cursive style with a large, stylized "K" and "F".

Kevin A. Foote  
Founder & CEO

### Activate ProtectMyID Now in Three Easy Steps

1. ENSURE That You Enroll By: **[date]** (Your code will not work after this date.)
2. VISIT the ProtectMyID Web Site to enroll: **[url]**
3. PROVIDE Your Activation Code: **[code]**

If you have questions or need an alternative to enrolling online, please call 877-288-8057 and provide engagement #: **[number]**

### ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identify Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **\$1 Million Identity Theft Insurance<sup>1</sup>:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

**Activate your membership today at [www.protectmyid.com/redeem](http://www.protectmyid.com/redeem)  
or call 877-288-8057 to register with the activation code above.**

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

### Additional Steps You Can Take

Even if you choose not to take advantage of this free credit monitoring, we recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free

---

<sup>1</sup> Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

*Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111

*Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742

*TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

*Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue, NW  
Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)





Interactive Healthcare

May XX, 2017

[First Name][Last Name]  
[Street Address]  
[City], [State] [Zip Code]

### **Notice of Data Breach**

Dear [First Name] [Last Name]:

FastHealth is a contracted vendor of [Healthcare provider]. We provide healthcare clients with operational and website services, including online bill-pay platforms. We are committed to protecting the security and confidentiality of our clients' and their patients' information. Regrettably, we are writing to inform you about an incident involving some of that information.

#### **What Happened**

On December 21, 2016, FastHealth discovered suspicious code on a server. Upon learning of this, we immediately began an investigation and hired a leading computer security firm to assist. On January 24, 2017, the computer security firm determined that an unauthorized third party altered code on FastHealth's web server that was designed to capture payment card information as it was being entered on FastHealth's online bill-pay platforms from January 14, 2016 to December 20, 2016.

#### **What Information Was Involved**

FastHealth's forensic investigation concluded on March 25, 2017, and we subsequently determined the information that may have been affected includes your name, billing address, email address, phone number, payment card number, expiration date and security code (CVV), and any comments or messages you included with your payment.

#### **What You Can Do**

We encourage that you remain vigilant to the possibility of fraud and identity theft by reviewing your financial statements for any unauthorized activity. You should immediately report any unauthorized charges to your financial institution because the major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges that are timely reported. The phone number to call is usually on the back of your payment card. You should also review the additional information on the following page on ways to protect yourself.

#### **What We Are Doing**

We sincerely apologize for any inconvenience or concern this may cause you. To help prevent something like this from happening in the future, we have removed the malicious code and continue to take steps to strengthen the security of our network.

**For More Information**

If you have any questions, please call 1-844-534-0814, Monday through Friday, from 9 a.m. to 9 p.m. EST (closed on U.S. observed holidays).

Sincerely,

A handwritten signature in blue ink, reading "Kevin A. Foote". The signature is fluid and cursive, with the first name "Kevin" and last name "Foote" clearly legible.

Kevin A. Foote  
Founder & CEO

### **MORE INFORMATION ON WAYS TO PROTECT YOURSELF**

We recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

*Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111

*Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742

*TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

*Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue, NW  
Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)